Kennedy NASA Procedural Requirements

Effective Date: **June 18, 2015**

Expiration Date: **June 18, 2020 (EXTENDED UNTIL MAY 18, 2021)**

Responsible Office: **Safety and Mission Assurance**

KSC System Safety and Reliability Analysis Procedural Requirements

National Aeronautics and Space Administration

John F. Kennedy Space Center

KDP-KSC-T-2120, Rev. Basic

Change Log

Date	Revision	Description
8/14/14	Basic-1	This document has been extended pending an extensive review and rewrite and to comply with NPR 1400.1, NASA Directives and Charters Procedural Requirements.
12/22/14	Basic-2	Administratively changed to extend expiration date. A longer review cycle is required due to the significance of the revision and to allow adequate time for all stakeholders to review the significant changes. The significant changes include making revisions to support the new KSC environment and to accommodate changes recently made to Agency documentation.
3/26/15	Basic-3	Administratively changed to extend expiration date due to the significance of revisions and to allow for processing of final signatures.
6/18/15	A	Kennedy NASA Procedural Requirements (KNPR) 8700.2 underwent a major revision to reorganize the content and to make the requirement statements concise, clearly identifying the subject of the requirement. KSC-UG-2812, KSC System Safety and Reliability Analysis Methodology User Guide, contains best practices, guidance, and helpful information to accompany this KNPR. Given the large rewrite, individual changes are not noted here in the revision history. Changes of note for this revision include: 1. Removal of duplicate requirements throughout. 2. Removal of design review milestones. These milestones are the purview of NPR 7120.5, NASA Space Flight Program and Project Management Requirements, NPR 7123.1 NASA Systems Engineering Processes and Requirements, and NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements. 3. Moved “how to” methodology and analyses templates to KSC-UG-2812. 4. Clarified requirement responsibilities (who is responsible for what) by using an active sentence structure. 5. Added information regarding tailoring.
5/19/20	A-1	Extension approved to allow for rewrite, Center wide review, comment disposition, and processing of final signatures.

12/16/2020	A-2	Additional extension due to loss of personnel working on the KNPR, addition of new hazard analysis methods, and development of new associated users' guide.

Table of Contents

List of Tables

PREFACE

P.1 PURPOSE

a. It is policy at John F. Kennedy Space Center (KSC) to provide and maintain safe and reliable systems that perform operations in a manner that minimizes risk. This document contains the system safety and reliability analysis requirements for systems at KSC. These requirements are consistent with applicable NASA system safety and reliability analysis policies, procedures, and standards and are intended to assist KSC in meeting system safety and reliability analysis goals.

b. The system safety and reliability analyses requirements contained herein will be used to identify and document hazards, hazard controls, Critical Items (CIs), and CI retention rationale; and to ensure that known hazards and CIs, and the residual risks are subjected to management review, approval/concurrence, or acceptance. The analyses are used to demonstrate the system meets established safety goals and thresholds.

c. When referring to reliability analyses, the purview of this document is limited to reliability analyses used to evaluate systems for degree of failure tolerance. Other reliability analyses such as maintainability analysis, logistics support analysis, reliability prediction, and probabilistic risk assessment are addressed in Kennedy NASA Procedural Requirement (KNPR) 8720.2, KSC Reliability & Maintainability Procedural Requirements.

d. KSC-UG-2812, KSC System Safety and Reliability Analysis Methodology User Guide is available as a supplement to this KNPR. It provides additional information to guide Civil Servant and contractor design or safety/reliability engineers during the performance of system safety and reliability analyses and includes information such as: analyses templates, special ground rules, procedures, and considerations that may be applied in the performance of the analyses, guidance regarding legacy analyses, special analysis considerations (flexible hoses, orifices, filters, computer tag analysis, etc.), generic hazards, rationale for the non-performance of a Criticality Assessment (CA) and Failure Modes and Effects Analysis (FMEA), Common Cause Failure Analysis (CCFA), and human error analysis.

P.2 APPLICABILITY

a. This directive is applicable to NASA Civil Servants and NASA contractors (including sub-contractors), as specified in their program plans or contracts, performing the safety and/or reliability analyses described herein for KSC systems.

b. Retroactive application of this directive to existing systems is not required. In special cases, this directive may be applied retroactively at the discretion of the applicable NASA contracting representative and NASA Safety and Mission Assurance (S&MA) manager.

c. In the event of a conflict between the requirements set forth in this document and:

(1) Agency or Program requirements, the Agency or Program requirements take precedence.

(2) Existing contract or documented agreement provisions, the contract or documented agreement provisions take precedence.

(3) Documents that are sub-tier to this KNPR, the provisions of this KNPR take precedence.

(4) Other documents at an equivalent level (e.g., other KNPRs), the respective document Offices of Primary Responsibility will resolve the conflict on a case-by-case basis and provide appropriate guidance.

d. If disagreement exists over which of the aforementioned documents take precedence, the Center S&MA Director shall make the final determination.

e. A closed-loop hazard tracking system is necessary to ensure that identified risks are mitigated to the levels accepted by the appropriate approval authority (NASA Procedural Requirement (NPR) 8715.3, NASA General Safety Program Requirements). Requirements for a closed-loop tracking system are beyond the scope of this KNPR. However, this KNPR provides the requirements for identifying safety risks and risk mitigations, and therefore, the closed-loop hazard tracking system should be closely coordinated with the requirements of this KNPR.

f. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term “shall.” The terms “may” or “can” denote discretionary privilege or permission, “should” denotes a good practice and is recommended, but not required, “will” denotes expected outcome, and “are/is” denotes descriptive material.

g. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

P.3 AUTHORITY

a. NPD 8820.2 Design and Construction of Facilities

b. NPR 7120.5, NASA Space Flight Program and Project Management Requirements

c. NPR 7123.1 NASA Systems Engineering Processes and Requirements

d. NPR 8715.3, NASA General Safety Program Requirements

P.4 APPLICABLE DOCUMENTS AND FORMS

a. KNPR 8715.3-1, KSC Safety Procedural Requirements Volume 1, Safety Procedural Requirements for Civil Servants/NASA Contractors

b. KNPR 8720.2, KSC Reliability & Maintainability Procedural Requirements

c. KNPR 8750.1, KSC Software Assurance Procedural Requirements

d. KSC-UG-2812, KSC System Safety and Reliability Analysis Methodology User Guide

e. Fault Tree Analysis Handbook with Aerospace Applications

P.5 MEASUREMENT/VERIFICATION

Compliance with the requirements contained in this KNPR will be verified through system safety and reliability analysis review activities performed by the NASA S&MA organization.

P.6 CANCELLATION/SUPERSESSION

This revision supersedes KNPR 8700.2, Rev. A-1, KSC System Safety and Reliability Analysis Methodology Procedural Requirements.

Approved By:

/original signed by Johnny Nguyen for/

_____

William Russ DeLoach
Director, Safety and Mission Assurance

Distribution: TechDoc Library

CHAPTER 1: GENERAL PROVISIONS

1.1 GOAL

The goal of this document is to provide KSC system safety and reliability analysis requirements that will optimize all aspects of safety and reliability within the constraints of operational effectiveness, time, and costs throughout all phases of the system life cycle.

1.2 OBJECTIVE

The objective of this KNPR is to document KSC system safety and reliability analysis requirements that can be tailored for use by KSC programs, projects, and the Institution.

1.3 RESPONSIBILITY

The Center S&MA Director is responsible for establishing a safety program that identifies and documents hazards, hazard controls, CIs, CI retention rationale, and ensures that known hazards and CIs are identified in a timely manner. This ensures risks are reduced to an acceptable level for operations and that the appropriate management review and approval/concurrence occurs.

CHAPTER 2: REVIEW AND APPROVAL PROCESS

2.1 Tailoring of this document is permitted if other analysis techniques will be used to satisfy the intent of the requirements set forth in this document or if the safety and reliability requirements in this document are met through program/project requirements. It is expected that much of the rationale for tailoring will already have been developed in retrievable program, project, or contractor records and can simply be referenced (in an appropriate, accessible form) in the tailoring documentation.

2.2 The level of tailoring documentation should be commensurate with the significance of departure from the norm. In the case where evaluation indicates that the tailoring of a requirement increases risk, evidence of official acceptance of the risk should be provided in retrievable program, project, institutional, or contractor records.

2.3 In the absence of a formally established review and approval process for safety and reliability analyses, the review and approval process herein shall be followed.

2.4 Analysts seeking the review and approval of risks identified in reliability and safety analyses shall:

a. Document and communicate the risk to the design team to ensure that the risk is mitigated to an acceptable level.

b. Communicate the risk to any impacted interfacing organizations.

c. Obtain (in order, as follows) the approvals from the responsible NASA Safety Engineer, the NASA Safety Engineer's Branch/Division Chief (or equivalent), the Ground Risk Review Panel (GRRP), the Center S&MA Director, and the Center Director (CD), up to the level required in Table A.

Note 1: The required approval level for safety and reliability analyses is dependent on the level of risk identified in the analyses. Each of the approval authorities listed above may not be required for every analysis. Thresholds for risk approval are located in Table A.

Note 2: These reviews are intended to ensure that the design is progressing in a manner that will mitigate risks to a level that is acceptable to the responsible S&MA authority.

Table A: Institutional Hazard Risk Approval Matrix

Likelihood							
	Very High	5	NASA S&MA Engineer	S&MA Director	CD	CD	CD
	High	4	NASA S&MA Engineer	GRRP	S&MA Director	CD	CD
	Moderate	3	NASA S&MA Engineer	NASA S&MA Engineer	GRRP	S&MA Director	CD
	Low	2	NASA S&MA Engineer	NASA S&MA Engineer	GRRP	GRRP	S&MA Director
	Very Low	1	NASA S&MA Engineer	NASA S&MA Engineer	NASA S&MA Engineer	NASA S&MA Engineer	GRRP
	Eliminated	E	Original Risk Approval Level Required				
			1	2	3	4	5
Green	Yellow	Red	Very Low	Low	Moderate	High	Very High
			Consequence				

d. The Institution shall use the KSC Risk Management Scorecard to communicate risks at the Center level.

Note: Risks identified through the performance of system safety and reliability analyses might not be communicated in a program, project, or Center risk system unless residual risk levels mandate the communication and disposition or acceptance of risk at these levels. It is necessary, however, to communicate hazards in terms of risk at the system level. Thus, a Hazard Risk Matrix is used (see Section 5.2 for additional information).

2.5 Requests for relief from the requirements of this document shall be in accordance with KNPR 8715.3-1, KSC Safety Procedural Requirements Volume 1, Safety Procedural Requirements for Civil Servants/NASA Contractors.

CHAPTER 3: GENERAL SYSTEM SAFETY AND RELIABILITY ANALYSIS REQUIREMENTS

3.1 NOMENCLATURE

3.1.1 The term “system” is used in this document to refer to both a system within an organizational hierarchy as well as the combination of elements/systems that function together to produce the capability required to meet a need. These terms and their use are defined below:

a. When referring to system organizational hierarchy, this document uses the following hierarchical naming convention in decreasing levels of complexity: Program, Project, element, system, subsystem, component, and Line Replaceable Unit (LRU). In this context, system is defined as the highest level of hardware organization composed of multiple subsystems.

b. When not referring to system organizational hierarchy, the term “system” is used to refer to the combination of elements that function together to produce the capability required to meet a need as defined in NPR 8715.3, In this context, the system elements include all hardware, software, equipment, facilities, personnel, processes, and procedures to meet this need.

3.1.2 In cases where the analysis techniques provided in this document are used in an application where another naming convention is used, the requirements contained within this document will be applied at the equivalent organizational hierarchy level (e.g., if a program uses “subsystem” to describe what this KNPR calls a “system,” the provisions of this KNPR should be applied at the subsystem level for that program.)

3.1.3 The term analyst is used throughout this document to refer to the Civil Servant or contractor personnel facilitating safety or reliability analyses.

3.2 GENERAL ANALYSIS REQUIREMENTS

3.2.1 System safety and reliability analysis templates shall be submitted to and approved by NASA S&MA prior to first use.

3.2.2 Analysts completing system safety and reliability analyses shall ensure that:

a. The applicable design and S&MA failure tolerance requirements are met.

Note: When failure tolerance requirements cannot be demonstrated, Design for Minimum Risk (DFMR) should be considered. DFMR criteria should be discussed with the design team and may need to be approved by NASA S&MA.

b. Analyses are applied throughout all phases of the system lifecycle.

c. Analyses are reviewed by NASA S&MA prior to design review milestones.

d. NASA S&MA comments are resolved prior to design reviews.

e. The analyses are delivered according to the design schedule.

Note: Expectations for analysis maturity level at each design milestone should meet the applicable design review entrance requirements or be negotiated with the appropriate project and S&MA organizations.

f. The analyses are reviewed and approved according to Chapter 2.

g. The analyses are placed under configuration control.

h. The analyses are maintained and periodically reviewed to ensure continuous reduction or elimination of risk.

i. The analyses are evaluated to determine if updates are required when form, fit, function, material, or operating environment (i.e., modified or repurposed) of the system changes.

Note: This includes instances when new hardware or software failure information becomes available or when legacy/repurposed systems are used to support new/different programs/projects.

3.2.3 Analysts shall input controls identified in hazard analyses, retention rational identified in CI Reports, and test and inspection methods identified in FMEA in a closed-loop hazard tracking system.

Note: Controls that require incorporation into operation, maintenance, or work authorization documents should be tracked. If these controls are changed, the analyses should be re-evaluated to ensure the hazards are sufficiently mitigated.

3.2.4 When the decision is made to use legacy safety and reliability analyses for a system, the analyst shall:

a. Document the rationale for using the analyses as-is or for updating the analyses.

b. Present the rationale prior to implementation to the appropriate program/project approval authority or to the GRRP for the Institution.

c. Enter applicable Hazard Report (HR) and the FMEA/CI Report information into the appropriate databases via the configuration management process.

3.2.5 Analysts using vendor-supplied system safety and reliability analyses shall:

a. Determine whether additional analysis may be necessary to supplement the vendor-supplied analyses to comply with the requirements of this KNPR.

b. Analyze the specific application of the Commercial Off-the-Shelf (COTS) if it is used outside its originally intended purpose.

3.2.6 When complementary safety and reliability analyses are performed for a system, analysts shall include the complementary analyses in a System Assurance Analysis (SAA) deliverable. Analyses which are published independently such as HRs, Operating and Support Hazard Analyses (O&SHAs), Ground Operations Risk Assessments (GORAs), and Software Assurance Classification Assessments (SACAs) need not be included in the SAA but may be referenced.

Note: If a Reliability and Safety Assessment Report (*RSAR) is conducted and it is the deliverable for the system per Chapter 4, it does not have to be incorporated into an SAA. When both system safety and reliability analyses are deemed appropriate for a system, the analyses are intended to complement each other. The SAA is intended to package the complementary analyses together into a cohesive analysis for the system.*

3.2.7 Analysts shall communicate findings to impacted interfacing critical systems throughout all phases of the system lifecycle.

CHAPTER 4: RELIABILITY AND SAFETY ANALYSIS REPORT

The RSAR is the first system safety and reliability assessment. The RSAR is a high-level, concept-of-operations assessment that defines the system's boundaries. Depending on the findings contained in the RSAR, additional analyses may be needed to support the design. Table B displays the types of analyses that may be required when certain system attributes are present as well as additional analyses that may be needed to further identify or refine hazards and/or critical functions.

Table B: Safety and Reliability Analysis Requirements

System Attributes (If)	Analyses (Then)	Required	When Needed*
The system does not have hazardous attributes or critical functions	RSAR is the system safety and reliability deliverable.	✓	
The system has hazardous attributes, but no critical functions The system has software	RSAR	✓	
	PHA	✓	
	FTA/HA		✓
	SHA		✓
	HR		✓
	JHA, O&SHA, or GORA		✓
	SACA	✓	
The system has hazardous attributes and critical functions The system has software	RSAR	✓	
	PHA	✓	
	FTA/HA		✓
	SHA		✓
	HR		✓
	JHA, O&SHA or GORA		✓
	CA	✓	
	FMEA, CI, End-to-End		✓
	SACA	✓	
The system has critical functions but does not have hazardous attributes. The system has software	RSAR	✓	
	CA	✓	
	FMEA/CI, End-to-End		✓
	SACA	✓	

* Analysts will obtain NASA S&MA approval prior to performing additional or more in-depth analyses.

Note 1: In some cases the RSAR will determine that system design and consensus standards control system risk and safety and/or reliability analyses will not be required.

Note 2: If complementary system safety and reliability analyses are performed for a system they will be consolidated into an SAA (see Chapter 7).

4.1 Analysts completing an RSAR shall:

a. Complete the RSAR as early in the system design as possible to determine/document system attributes and specify the depth of analysis required.

b. Assess the system to determine whether it has hazardous attributes (safety critical).

c. Assess the system to determine if loss or improper function of the system could result in a Level 4 or Level 5 severity per Section 5.2.1 (mission critical).

Note: The analyst uses the high-level system description and concept of operations to determine the basic function(s) of the system. Depending on the program, project, or institutional performance requirements for the system, reliability analyses may not need to be performed. Loss or improper performance of a system may be considered an acceptable risk based on established risk thresholds and the intended use of the system.

d. Identify system design and consensus standards and determine whether they control the potential risk identified in b. and c. above.

Note: The analyst will work with the design team to evaluate whether design and consensus standards provide adequate control of the risk. If it is determined that design and consensus standards control the risk no further analysis is needed. Additional safety and/or reliability analyses may be required depending on the application, function, or when a system is used in a way other than that for which it was designed (i.e., repurposed).

The following are a few examples of systems that meet consensus standards which may not need additional safety and reliability analyses:

(1) Conventional facilities (i.e., office buildings) and utilities (e.g., City of Cocoa Water Supply)

(2) COTS equipment (e.g., tools, grounds-keeping equipment, General Services Administration vehicles, medical equipment, standard fire trucks)

(3) Facility maintenance equipment

(4) Lightning protection systems

(5) Facility fire protection and detection systems

(6) Elevators

e. Identify whether the system contains software.

4.2 If the analyst determines that a system does not have hazardous attributes or critical functions, the RSAR shall serve as the system deliverable.

4.3 When the RSAR serves as the system deliverable and the system changes form, fit, function, material, or operating environment (i.e., modified or repurposed), the analyst shall review the RSAR to determine if the changes introduce hazards or critical functions which would require an update to the RSAR or additional analyses.

4.4 If the analyst determines that the system has hazardous attributes (safety critical) and design and consensus standards do not control the risk, the analyst shall recommend a Preliminary Hazard Analysis (PHA) be performed to identify hazards, their causes and effects, and recommend hazard elimination or mitigations/controls. See Section 4.0 Safety Analysis.

4.5 If the analyst determines that loss or improper function of a system could result in a Level 4 or Level 5 severity per Section 5.2.1 (mission critical) and design and consensus standards do not control the risk, the analyst shall recommend that a CA be performed. See Section 6.1 Criticality Analysis.

4.6 If the analyst determines the system is critical (safety critical or mission critical) and it contains software, the analyst shall coordinate with the software assurance analyst to ensure a SACA is performed in accordance with KNPR 8750.1, KSC Software Assurance Procedural Requirements.

4.7 Analysts performing a RSAR shall obtain NASA S&MA approval prior to performing additional or more in-depth analyses.

CHAPTER 5: SYSTEM SAFETY ANALYSIS

System Safety is the application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle. The PHA is used during the conceptual design phase to identify hazards at a high level. Depending on the complexity of the system, the PHA may be further developed into a Fault Tree Analysis (FTA)/Hazard Analysis (HA) or into a System Hazard Analysis (SHA). Additionally, it may be determined that alternative types of safety analyses such as a Job Hazard Analysis (JHA), an O&SHA, or a GORA may be needed. The type of analysis performed is dependent on the system and its operation, procedures, the environment, and location.

5.1 HAZARD REDUCTION ORDER OF PRECEDENCE

The overall goal of system safety is to design systems that do not contain hazards. However, the nature of complex systems makes it impossible or impractical to design systems that are completely hazard-free. The hazard reduction order of precedence defines the order to be followed for satisfying system safety requirements and reducing risks to an acceptable level.

5.1.1 Analysts shall use the following hazard reduction order of precedence during the design process to ensure that system hazards are eliminated or controlled:

Note: Some hazards may require a combination of the following approaches to mitigate a potential hazard to an acceptable level of risk.

a. Eliminate the hazard by design.

b. Design for minimum hazards by:

(1) Designing systems to be fail-operational/fail-safe combinations and including safety factors to ensure inherent safety through selection of design features.

(2) Implementing damage control, containment, and isolation of potential hazards where possible to ensure control and mitigation is built into each design.

c. Incorporate Safety Devices - Known hazards which cannot be eliminated through design or mitigated to acceptable levels will be reduced to an acceptable level through the use of safety devices (e.g., guards, interlocks, etc.) as part of the system, subsystem, or equipment.

d. Provide caution and warning devices for the timely detection of the condition (e.g., oxygen monitors) and the generation of distinguishable warning signals.

e. Develop and implement administrative controls (e.g., special procedures, training, administrative barriers, signs) using standardized notation for all precautions.

f. Personal Protective Equipment.

5.2 THE RISK MATRIX

Risk thresholds and guidelines may vary by program, project, or the Institution. The hazard risk thresholds and requirements in this document apply to institutional hazard analyses and hazard reports and are applicable to programs and projects when likelihood and consequence criteria for assessing risks have not been defined.

5.2.1 Hazard Severity

5.2.1.1 Analysts shall assess all hazard effect(s), including worst-case effects.

5.2.1.2 Analysts shall determine the initial hazard severity without taking into consideration hazard mitigations/controls.

5.2.1.3 Analysts shall use the following hazard severity classifications when assessing the hazard effects for the Institution or when no classification exists:

a. Severity 5 – Very High. A hazard condition that may cause loss of life or permanent total disability (may be classified as a Type A Mishap); loss of facilities, systems, or equipment essential to KSC's mission, loss of flight hardware; or a catastrophic environmental release or formal Environmental Protection Agency (EPA) enforcement action with major penalty and/or criminal investigation.

b. Severity 4 – High. A hazard condition that may cause permanent partial disability (may be classified as a Type B Mishap); major property damage to facilities, systems, or equipment essential to KSC's mission, major damage to flight hardware; major release to the environment or formal EPA violation with minor penalty.

c. Severity 3 – Moderate. A hazard condition that may cause long-term, severe injury, impairment, or incapacitation (may be classified as a Type C Mishap); moderate property damage to facilities, systems, or equipment essential to KSC's mission, moderate damage to flight hardware; significant release to the environment, possible formal EPA enforcement action with possible penalty.

d. Severity 2 – Low. A hazard condition that may cause short-term, minor injury, impairment, or incapacitation (may be classified as a Type D Mishap); minor property damage to facilities, systems, or equipment essential to KSC's mission, minor damage to flight hardware; minor release to the environment, warning letter or self-reportable EPA violation without penalty.

e. Severity 1 – Very Low. A hazard condition that may cause the need for minor first aid (may be classified as a Close Call); that subjects facilities, systems, equipment, or flight hardware to more than normal wear and tear; insignificant release to the environment, negligible or non-reportable EPA violation.

5.2.2 Hazard Likelihood

5.2.2.1 Analysts shall evaluate the likelihood (i.e., probability of occurrence) that an identified hazardous effect (consequence/severity) will occur from the identified cause.

5.2.2.2 Analysts shall assess the likelihood of the hazard occurring for the projected usage/life of the system.

5.2.2.3 Analysts shall use the following likelihood classifications when assessing the likelihood of a hazard for the Institution or when no classification exists for a program or project:

> *Note: When quantitative probability data is available, the analyst should use the probability criteria defined by the program/project/Center scorecard to determine the corresponding likelihood level.*

a. Likelihood Level 5 – Very High. Highly likely to occur. Existing controls have little or no effect and cannot prevent the hazard; no alternative controls are available.

b. Likelihood Level 4 – High. Likely to occur. Existing controls have significant limitations and/or uncertainties and will likely not prevent the hazard; additional actions will be required.

c. Likelihood Level 3 – Moderate. Could occur. Existing controls have some limitations and/or uncertainties and may prevent the hazard; additional actions may be required.

d. Likelihood Level 2 – Low. Unlikely to occur. Existing controls have minor limitations and/or uncertainties and are usually sufficient to prevent the hazard; some additional actions may be required.

e. Likelihood Level 1 – Very Low. Highly unlikely to occur. Existing controls are strong and are expected to prevent the hazard.

Note: Hazards with a likelihood of 1 are considered controlled hazards.

f. Likelihood Level E – Eliminated. The hazard no longer exists.

Note: Hazards are considered eliminated when they have been designed out, either through an alternative design option or through modification of the existing design.

5.2.3 Hazard Risk Matrix

5.2.3.1 Analysts shall use the Hazard Risk Matrix in Table C to communicate risk associated with hazards identified in safety and reliability analyses for the Institution's systems or when a risk matrix is not defined for a program or project.

5.2.3.2 Analysts shall determine the risk score as the likelihood level multiplied by the consequence/severity level (e.g., 1 x 5 = 5, 2 x 4 = 8, etc.).

Table C: Hazard Risk Matrix

Likelihood							
	Very High	5					
	High	4					
	Moderate	3					
	Low	2					
	Very Low	1					
	Eliminated	E					
			1	2	3	4	5
Green	Yellow	Red	Very Low	Low	Moderate	High	Very High
			Consequence				

5.3 PRELIMINARY HAZARD ANALYSIS

The PHA is used to (1) further develop system safety requirements, (2) prepare performance/design specifications, (3) develop the preliminary hazard mitigations/controls, and (4) initiate the hazard tracking and risk resolution process.

5.3.1 Analysts conducting a PHA shall:

a. Determine the hazards, hazard causes, and hazardous effects associated with the system.

b. Identify hazard cause(s) to the level at which the associated hazard can be eliminated by design or controlled to an acceptable level of risk.

c. Assess each hazard cause and effect combination to determine the consequence/severity per Section 5.2.1.

d. Assess each hazard cause and effect combination to determine the likelihood of occurrence per Section 5.2.2.

e. Identify the initial safety requirements for eliminating, reducing, and/or controlling the identified risk.

f. Assess the hazard and its associated controls for the specific time(s) when the hazard is present as well as those times when the hazard may not manifest.

> *Note: Depending on the function of the system a hazard may not present itself for the full operational period, therefore, controls may only be necessary for the time period that the hazard could occur.*

g. Document software hazards, hazard causes, preliminary effects, and preliminary hazard mitigations/controls.

5.3.2 Depending on the results of the PHA, the analyst shall seek approval for additional or more in-depth analyses.

> Note: Additional or more in-depth hazard analyses generally follows the PHA with a SHA, FTA/HA, or an O&SHA, as appropriate. For some programs or projects the PHA will suffice as the formal deliverable.

5.4 FAULT TREE ANALYSIS

FTAs provide a top-down, deductive reasoning, failure analysis in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events. The type and depth of analysis required for each FTA may vary depending on the complexity of the system and its criticality; however, an FTA of an operational system failure is typically developed to a major component or contributor level (valves, pumps, identifiable human errors, etc.).

5.4.1 Analysts shall use the “Fault Tree Analysis Handbook with Aerospace Applications” to perform the FTA technique that applies to the system that is being analyzed.

5.4.2 Analysts performing FTAs shall:

a. Identify hazards associated with the system, including hazards associated with operating conditions.

b. Designate a clearly-defined undesired event as the topmost event of the FTA, ensuring that the scope is limited enough to accurately represent all the possibilities or conditions necessary to cause it.

Note: The topmost event is typically defined as: Injury/loss of life, loss of/damage to a system, loss of/damage to flight hardware, or environmental impact.

c. Define intermediate events (i.e., those below the top-level event) by the immediate, necessary, and sufficient causes that led to the top-level event.

d. Evaluate state of component faults for primary, secondary, and command faults.

e. Identify the following hazard causes in the FTA at a minimum:

(1) Hardware failure modes

(2) Personnel actions or inaction

(3) Software hazard causes

(4) Component interactions

(5) Environmental condition(s) (induced or natural)

(6) Inherent system hazards

f. Include sufficient detail to provide a logical trail from the topmost event through the intermediate events, to the basic events (i.e., cause level) which could include FMEA failure modes, and if applicable, failure mode causes.

g. Develop the FTA to a depth that will identify all hazardous conditions/events and all credible corresponding causes with sufficient detail to document the following in the corresponding HA:

(1) Methods to eliminate the hazard

(2) Controls that mitigate the hazard to an acceptable level

(3) FMEA failure modes or failure mode causes (if corresponding)

(4) Software hazard causes and controls

5.4.3 Analysts shall document the results of the FTA in an HA.

5.4.4 Analysts shall use CCFA to determine/identify common events or causative mechanisms that can result in multiple failures of redundant (like or unlike) components or operator error.

5.4.5 Analysts shall take into account human error when performing the FTA and document the findings in the HA.

5.5 HAZARD ANALYSIS

The general purpose of the HA is to continue the maturation of the system safety analysis at a more detailed level than in a PHA. The HA is used in conjunction with a FTA to provide additional details on how the undesirable topmost event may occur. All hazards inherent to the system should be understood well enough to finalize the FTA/HA by the Critical Design Review (CDR).

5.5.1 Analysts conducting an HA shall meet the same requirements as those completing PHAs (per Section 5.3).

5.5.2 In addition, analysts performing an HA shall:

a. Identify or refine and document hazards associated with the system.

b. Include causes identified in the FTA.

c. Document the details of hazard controls and the verification of controls.

d. Document the verification of the system's compliance with design and safety requirements.

e. Reference the document number or incorporate corresponding software analyses performed on critical software.

> *Note: Software analyses performed per* KNPR 8750.1, KSC Software Assurance Procedural Requirements *should be referenced or incorporated into the FTA/HA.*

f. Reference integrated hazards.

g. Communicate hazards, hazard causes, hazard controls, and hazard effects that cross one or more systems or elements to the next higher level than that in which it was identified to ensure they are documented in an Integrated Hazard Analysis (IHA) (see Section 5.8).

h. Explain how the potential for a single event or a CCFA which can remove more than one inhibit to a potentially hazardous event are eliminated by meeting the failure tolerance requirements.

5.5.3 Analysts shall develop HRs as directed by Section 5.7 to the maximum extent allowed by the definition of the design.

> *Note: HRs are only required when the hazard risk exceeds the risk acceptance thresholds as defined in Section 5.7.*

5.6 SYSTEM HAZARD ANALYSIS

The general purpose of the SHA is to continue the maturation of the safety analysis of a system at a more detailed level than that provided in a PHA when an FTA is not required. As more information about a system becomes available throughout the design process, the safety analysis should be further matured, and any assumptions made during the performance of the PHA should be verified. All hazards inherent to the system should be understood well enough to finalize the SHA by the CDR.

5.6.1 Analysts conducting SHAs shall meet the same requirements as those completing PHAs (per Section 5.3).

5.6.2 In addition, analysts conducting SHAs shall:

a. Reference the document number or incorporate software analyses performed on safety-critical software.

Note: Software analyses performed per KNPR 8750.1, KSC Software Assurance Procedural Requirements should be referenced or incorporated into the SHA.

b. Refine hazards, hazards causes, hazardous effects, and hazard controls identified in the PHA by adding specific details.

c. Document the verification of the system's compliance with design and safety requirements.

5.6.3 Analysts shall develop HRs as directed by Section 5.7 to the maximum extent allowed by the definition of the design.

Note: HRs are only required when the hazard risk exceeds the risk acceptance thresholds as defined in Section 5.7.

5.7 HAZARD REPORTS

HRs document mitigation(s)/controls for potential hazards identified in the FMEA, FTA/HA, and the SHA. The HR allows management to make an informed decision to proceed or not based on the risk level. The following requirements are intended for hazards reports associated with the Institution's systems and industrial hazards associated with program systems.

5.7.1 Analysts developing HRs shall:

a. Include all hazards identified in the HA or SHA that have risk scores of 10 or higher on the Hazard Risk Matrix (Section 5.2, Table C).

Note: Hazards that have a risk score outside of the scores listed may require HRs due to factors such as high visibility, high cost, schedule impact, or one-of-a-kind item, etc.

b. Include a well-defined, specific hazard title which captures the unique hazard; and if site specific, the location of the hazard.

c. Identify the affected element to which the hazard is applicable (e.g., industrial, flight, ground operations, etc.).

d. Identify the location(s) that the hazard could impact.

e. Provide a description of the hazardous condition which fully defines the following:

(1) The scenario and hazard causes that must be controlled.

(2) Local, intermediate, and the worst-case effects or results of the hazard cause.

Note: If the hazard is for off-nominal conditions, annotate the assumptions that were made.

f. Provide a summary of the rationale for risk acceptance, elimination, or control.

g. Provide justification for the hazard likelihood including assumptions, any empirical data, uncertainties, confidence factors, and a qualitative summary of the failure history, limitations, or uncertainties in the controls that provide the basis for establishing the likelihood of the hazard occurring.

h. Provide a concise summary of the hazard risk scores for each hazard cause.

Note: This can be accomplished in many ways. The summary can be depicted using a hazard risk matrix in the HR which shows where each hazard cause lies on the matrix or it could be a summary listed in a tabular format.

i. Provide references to associated documentation including:

(1) Other HRs

(2) Integrated Hazards

(3) FMEA/CI Report information

(4) Operations related documentation (e.g., ground processing requirements, flight rules, Launch Commit Criteria)

j. Identify system interface(s) that cause or control hazardous conditions within the report.

k. Provide descriptions of the existing high-level safety requirement(s) necessary to mitigate the hazard. Include references to the document number and indicate to which causes or controls within the report the safety requirement applies.

l. For each hazard cause, include the following:

(1) Reference to the FTA (if applicable)

(2) Detailed description of the specific hazard cause being evaluated.

(3) Hazardous effects resulting from the hazard cause

(4) Likelihood of occurrence

(5) Consequence severity

(6 Hazard controls

(7) Verifications to ensure controls are implemented

m. Classify HRs as either:

(1) “Closed” when actions to control the hazard have been implemented or incorporated (e.g., design change incorporated; procedure and plans released) and verification of implementation or incorporation has been completed.

(2) "Open" if further action(s) to control the hazard is required (e.g., analysis, test, or verification of incorporation of the control).

(3) "Accepted" if upon approval any risk has a likelihood greater than Level 1 on the Hazard Risk Matrix.

(4) "Controlled" if upon approval all risks have a likelihood of Level 1 on the Hazard Risk Matrix.

(5) "Eliminated" if upon approval all risks have a likelihood of Level E on the Hazard Risk Matrix.

5.8 INTEGRATED HAZARD ANALYSIS

An IHA identifies hazards across system and organizational interfaces. An IHA includes the delineation of responsibilities at the cause level and the technical coordination of integrated hazards across elements to ensure completeness, establish an integrated effort, and to avoid overlaps and conflicts among the technical disciplines.

5.8.1 Management shall determine who is responsible for performing an IHA when hazards, hazard causes, hazard controls, and hazard effects cross elements (i.e., system or organizational boundaries).

5.8.2 Analysts performing an IHA shall:

a. Identify the integrated hazards associated with systems that crosses elements.

b. Identify hazard causes and document cause ownership.

c. Document the details of hazard controls and verifications, including ownership.

d. Reference corresponding FMEA and CI document numbers.

5.9 OPERATING AND SUPPORT HAZARD ANALYSES

The general purpose of the O&SHA is to perform a detailed safety risk assessment of a system's operational and support procedures to determine if the operational hazards are eliminated, mitigated, controlled, accepted, or open. The O&SHA identifies hazards and recommends risk reduction alternatives in procedurally controlled activities during all phases of system hardware and software use. The O&SHA is developed with the intent of establishing a systematic review and documentation of the operations, broken down into incremental parts and consistently analyzed for hazards.

5.9.1 Management shall determine whether an O&SHA should be performed when any of the following conditions exist:

a. The procedure is considered hazardous per KNPR 8715.3-1, KSC Safety Procedural Requirements Volume 1, Safety Procedural Requirements for Civil Servants/NASA Contractors.

b. The procedure has the potential to expose personnel/hardware/facility to hazards.

c. The procedure has never been performed.

d. There is a significant departure from standard operating procedure.

e. There has been a loss of tribal knowledge or personnel are inexperienced with the procedure.

f. The procedure uses new or modified equipment.

g. The process is complex or sensitive enough that evaluating the procedural tasks in detail would be value added.

h. An incident (mishap or close call) occurred during the procedure or a similar procedure.

i. A process escape has occurred during the process or a similar process.

5.9.2 When an O&SHA is directed, the analyst shall form an O&SHA team with the subject matter experts necessary to complete a thorough evaluation.

5.9.3 The O&SHA team shall:

a. Generate a formal report.

b. Evaluate the following:

(1) Human-induced hazards to personnel, hardware, software, equipment, facilities, and the environment (including unplanned events).

(2) Hazards resulting from hardware, software, equipment, facilities, commodities, and the environment.

(3) Hazards resulting from the installation, operations or tasks.

(4) Planned system configurations at each phase of activity.

(5) Facility and system interfaces.

(6) All possible environments throughout the process or operation.

(7) Supporting tools or other equipment used during the procedure.

(8) Operation or task sequence, the effects concurrent or parallel tasks, and their limitations.

(9) Regulatory or contractually specified personnel safety and health requirements.

c. Identify the potential hazards, hazard causes, and hazardous effects associated with the proposed operation in explicit detail.

d. Assess each hazard, at the lowest operational/procedure level, using the worst-case consequence/severity and likelihood.

e. Use the applicable risk scorecard to assess and score hazards that are identified in the O&SHA.

Note: The risk scorecard used to assess the risk associated with hazards identified in the O&SHA is dependent on the complexity of the operation and potential management visibility. The O&SHA team may choose to use a program, project, or Center risk scorecard.

f. Identify and reference the document number(s) for each hazard control.

Note: Hazard controls identified in the O&SHA should be input into a closed-loop hazard tracking system.

g. Identify hazard verifications for each hazard control.

5.10 GROUND OPERATIONS RISK ASSESSMENT

The general purpose of the GORA is to perform a high-level safety risk assessment of a specific process or to compare the risks of multiple methods of completing a process to identify hazards, recommend risk reduction alternatives to the process, and to facilitate risk-informed management decisions.

5.10.1 Management shall determine whether a GORA should be performed when any of the following conditions exist:

a. The safety risk or hazard assessment of a process is needed, but at a high level and not at a detailed task/step level (e.g., a process might be early in development and the detailed steps or hazard information may not yet be complete).

b. There is more than one method to complete a process and the risks of the various options need to be compared.

c. The process is considered hazardous per KNPR 8715.3-1, KSC Safety Procedural Requirements Volume 1, Safety Procedural Requirements for Civil Servants/NASA Contractors.

d. The process has the potential to expose hazards to personnel/hardware/facility.

e. An incident (mishap or close call) occurred during the process or a similar process.

5.10.2 When a GORA is required, the analyst shall organize a GORA team with subject matter experts necessary to produce a thorough evaluation.

5.10.3 The GORA team shall:

a. Generate a formal report.

b. Identify the risk scenarios associated with the proposed operation(s).

c. Identify the applicable scorecard to assess and score hazards.

Note: GORA's for the Institution should use the KSC Risk Management Scorecard*.*

d. Assess each risk scenario using the worst-case consequence/severity and likelihood for all severity categories.

e. Identify risk mitigations.

CHAPTER 6: RELIABILITY ANALYSES

6.1 CRITICALITY ASSESSMENT REQUIREMENTS

The CA is performed to identify the functions of all inputs and outputs of a system to determine whether a loss or failure of that function would be critical or non-critical. If a system has critical functions, the system is considered to be critical. For functions that are critical, a component FMEA is performed to further determine and analyze the criticality and effects of the failure.

6.1.1 Analysts performing the CA shall:

a. Use the most current system configuration.

b. Construct a System Functional Block Diagram that includes the following:

(1) All system inputs and outputs, including software inputs and outputs.

Note: System identification numbers (e.g., Program Model Numbers (PMNs)) should be labeled.

(2) An illustration showing the relationship between subsystems if the system is composed of multiple subsystems (e.g., multiple PMNs).

(3) Interfacing systems.

c. Describe each system function to determine the effects of loss or improper performance of the function.

d. Identify each unique timeframe in which the system's inputs and outputs are being analyzed.

e. Assess the following scenarios disregarding redundancy, mitigations/controls, emergency systems or contingency and emergency operations when determining the effects of loss or improper performance of the function:

(1) Premature operation

(2) Failure to operate at a prescribed time

(3) Failure during operation (including degraded or excessive performance)

(4) Failure to cease operation at a prescribed time

f. Designate functions as critical when the loss or improper performance of the function can result in a Level 4 or 5 consequence per Section 5.2.1.

g. Reference software analyses for the critical functions of the system.

6.1.2 Analysts shall perform a component FMEA when one or more input or output functions are identified as critical.

Note: The component FMEA is performed only on the components that contribute to the critical functions of a system.

6.1.3 Analysts shall complete a system End-to-End Review when one or more input or output functions are identified as critical.

6.2 FAILURE MODES AND EFFECTS ANALYSIS REQUIREMENTS

The component FMEA is a bottom-up, inductive reasoning, approach used to analyze a system's components to determine the worst-case effect(s) of the failure modes that contribute to a critical function of that system. Development of the component FMEA should be a collaborative effort between reliability, operations, and design engineering throughout the design phases to determine if the design has single-failure-points (SFPs), CIs, and meets failure tolerance requirements. Failure causes should be developed to a level of detail that allows requirement development for inspection, maintenance, and test planning in order to preclude or minimize the likelihood of occurrence of the failure cause for each credible failure mode that could result in a CI Report.

Because of the complexity and unique mission of some systems and operations, special ground rules, procedures, and considerations may be applied in the performance of the component FMEA. To assist the analyst, in addition to the requirements specified below, a collection of special considerations for several cases is located in KSC-UG-2812, KSC System Safety and Reliability Analysis Methodology User Guide.

6.2.1 General Failure Modes and Effects Requirements

6.2.1.1 Analysts developing component FMEAs shall:

a. List all active components for each critical function identified in the CA.

Note: Passive components are components that may be necessary to the performance or structural integrity of the system but have no active function. Thus, passive components need not be analyzed in the component FMEA. However, if at any time a component is actively used during an operation, it should be considered an active component (e.g., a manual valve that is turned by an operations engineer or technician during an operation).

b. Describe each component's function.

c. Analyze the components for every credible failure mode during all applicable time periods.

d. Describe any non-credible failure modes and obtain approval from the GRRP or appropriate program/project approval authority.

Note: Failure modes are designated as non-credible when the probability of an item failing in the critical mode is 10^{-6} or less for the projected usage/life of the equipment.

e. Perform the following for software associated with the system:

(1) Identify software failures as a failure cause where appropriate.

(2) Identify when Prerequisite Logic, Reactive Control Logic, Programmable Logic Controllers (PLC), or other relevant software is a mitigation for potential failure effects.

(3) Analyze PLCs in conjunction with the associated system controlled by the PLC.

f. Analyze the design to identify and eliminate or control Common Cause Failures (CCFs) for critical functions that employ like or unlike redundancy in the design.

g. Determine and describe the worst-case failure effects on system performance, personnel safety, and interfacing systems for each component that contributes to a critical function.

h. Analyzing across interfaces to determine the worst-case effects of failures that can propagate through the system and between subsystems.

Note: Consideration needs to be given to system interfaces for critical failures that can propagate at the system level. See Section 6.4 (End-to-End Review).

i. Identify the Criticality Category per Section 6.2.1.

Note: Critical components that cannot be eliminated by design will be documented as a CI Report and placed in the CIL.

j. Perform the Failure Tolerance Screens for all components being analyzed in the FMEA.

k. Conduct the FMEA within the component/LRU if the component/LRU does not pass the Failure Tolerance Screen and the component/LRU may have internal failure tolerance capability.

l. Identify and document potential failure causes for all Criticality Categories other than Crit. 3.

6.2.1.2 Analysts shall perform a FMEA on flexible hoses, orifices, and filters assessed as critical in the CA.

6.2.1.3 Analysts shall coordinate FMEA results with related safety analyses results (including software).

6.2.2 Criticality Categories

Criticality categories are a relative measure of the consequences of a failure mode. They are a reliability tool that assesses the priority of catastrophic events by taking into account redundancy (or the lack of redundancy). The criticality of a component is determined by S&MA analysis of the design, function, and application of the equipment.

6.2.2.1 Analysts assigning Criticality Categories in FMEAs shall:

a. Assign the initial criticality category for a failure mode based on the worst-case potential failure effect assuming the loss of all redundancy (i.e., 1, 2, or 3).

b. Assess the initial criticality category for redundancy and annotate based on the available design redundancy to yield the final criticality category (e.g., if one redundant leg is available, a criticality category 1 becomes a 1R2)).

c. Assign the Criticality Categories as follows (in order of worst-case precedence) when criticality category definitions have not been defined:

Note: Criticality categories are pre-defined risk thresholds used to identify the effect of loss or improper performance of a component. Early identification, tracking, and control of critical items through the preparation, implementation, and maintenance of CILs provides

valuable inputs to design, development, and operations. From the CIL activity, critical design features, tests, inspections, and procedures can be identified and implemented that will minimize the probability of failure for systems determined to be critical to the mission for which it was designed.

(1) Criticality Category 1: Single failure that could result in loss of life, loss of flight vehicle, or loss of a system essential to KSC's mission.

(2) Criticality Category 1R#: Redundant hardware items, which if all failed, could result in loss of life, loss of flight vehicle, or loss of a system essential to KSC's mission. A number (#) is used to indicate the number of failures required for the Level 5 consequence/severity effect (e.g., 1R2 for a single failure tolerant system; 1R3 for a two failure tolerant system).

(3) Criticality Category 1S: Single failure in a safety or hazard monitoring system that could cause the system to fail to detect, combat, or operate when needed during the existence of a hazardous condition and could result in loss of life, loss of flight vehicle, or loss of a system essential to KSC's mission. Safety criticality is designated with the notation "S" added to the Criticality Category.

(4) Criticality Category 2: Single failure that could result in severe injury to personnel, loss of mission, damage to a flight vehicle system, or major damage to a system essential to KSC's mission.

(5) Criticality Category 3: All other failures.

Note: If criticality category 1, 1S, 1R#, or 2, pass the Failure Tolerance Screens in Section 6.2.2, they will not require a CI Report.

d. Assign criticality with the assumption that nominal ground crew actions will be performed to activate standby redundant items, as long as detectability and time to effect criteria are met.

e. Indicate if the first failure of criticality category 1R# item can cause hazardous effects.

6.2.3 Failure Tolerance Screens

6.2.3.1 Analysts performing a component Failure Tolerance Screens shall:

a. Evaluate all redundant paths for redundant items.

b. Assess components on a PASS/FAIL basis using the following criteria:

(1) Screen A - The item is functionally verified during normal ground processing.

(2) Screen B - The health and status of the item is monitored or verified (failures are readily detectable by a system or personnel), and correcting action exists such that the time to detect and time to correct is less than the time to effect.

Note: For redundant items that have more than two redundant paths and one path fails Screen B, Screen B will be shown as FAIL unless detectability exists for the remaining paths such that failure tolerance is verifiable. For example, if the first failure in a three path system is not detectable, but the remaining two paths are capable of being monitored or verified, Screen B should be shown as "PASS."

(3) Screen C - The loss of all redundant hardware items cannot be the result of a credible CCF.

Note: Non-redundant items should be shown as Not Applicable (N/A) for Screen C.

c. Use the following terminology and criteria for Screen B when describing time-to-effect, time-to-detect, and time-to-correct timeframes (programs and projects may have different criteria):

(1) Immediate – less than 1 second

Note: A time scale (e.g., milliseconds) for software to detect a failure and to initiate corrective action should be documented.

(2) Seconds – 1 to 60 seconds

(3) Minutes – >60 seconds to 60 minutes

(4) Hours – >60 minutes to 24 hours

(5) Days – >24 hours to mission complete

d. Assign Critical Item Categories in accordance with Section 6.2.1.

e. Complete CI Reports as indicated by Section 6.3.

6.2.3.2 Analysts shall specify in the FMEA:

a. The reference to test, inspection, and operational use documentation that allows the item to pass Screen A and B.

b. Details on the expected or required software response to hardware failures if, through the use of software, the system provides for failure isolation and recovery from faults that affect critical functions.

6.3 CRITICAL ITEMS LIST REQUIREMENTS

The CI Report (or CI Sheet) contains specific rationale that justifies the retention of the CI in the system. The CI Report, via the retention rationale, identifies the inspection, process control, monitoring, and test/verification requirements for the CIs, and influences operations planning (including mission planning, procedure development, and logistical and maintenance support requirements). All CIs will be incorporated into a Critical Items List (CIL) database, which is used to document all CIs.

6.3.1 Analysts completing CI Reports shall:

a. Document components identified as criticality category 1, 1S, 1R#, and 2.

Note: Criticality category 3 does not require a CI Report.

b. Include all CIs Reports in a CIL database.

c. Document in the FMEA any residual risk resulting from a failure mode which has controls identified in the CI Report.

Note: This is to ensure that any residual risk from a failure mode that has controls with limitations is assessed in the FMEA.

d. Develop CI Report retention rationale to:

(1) Document the design, testing, inspection, and operational use that minimizes the failure mode's probability of occurrence.

(2) Describe any operational constraints or work-a-rounds as a result of the failure mode.

(3) Identify in explicit language all component attributes that must be verified.

(4) Address design, testing, inspection, operational use, failure history, and waivers and provide quantitative evidence of reliability or reference documents that contain this evidence.

(5) Identify any expected or required software response to the hardware failure.

(6) Describe corrective actions, including any action, automatic or manual, which is available to mitigate or prevent the effects of the failure, including any alternative means of accomplishing the function performed by the LRU/item or its assembly.

6.4 END-TO-END REVIEW REQUIREMENTS

An End-to-End Review crosses system boundaries to determine if interactions between all systems whose functional failures are critical or non-critical are captured. The End-to-End Review considers all critical function interdependencies of systems, including systems that are the design responsibility of other organizations, contractors, or centers. Definitions of upstream and downstream systems are provided in Appendix A.

6.4.1 Analysts conducting an End-to-End Reviews shall:

a. Review from end-to-end all direct and indirect interfacing systems to identify whether they contribute to or may impact the system's critical functions, regardless of boundaries between organizations, contractors, or centers.

b. Verify that interfacing systems input/output function(s) criticalities are consistent with the criticality assigned to the related input/output function(s) of the system or subsystem being analyzed.

c. Document any areas of concern in the SAA when inconsistencies with an interfacing system's input/output function criticality are identified.

d. Provide critical output function information to the applicable design and safety engineers for interfacing systems.

CHAPTER 7: SYSTEM ASSURANCE ANALYSIS

The SAA is a consolidation of the system safety and reliability analyses performed for a system. It is not the intent of the SAA to drive the types of analyses that are required (i.e., the RSAR is the analyses driver). The SAA is simply the official technical record that combines the various S&MA analyses for the specific design and use of a system into one document. It contains the technical rationale for how a system meets safety and reliability requirements, failure tolerance, and risk management thresholds. The reliability engineer and the safety engineer will need to discuss the results of the analyses to determine if any CIs or hazards may have been overlooked and to determine if they have implemented conflicting or excessive mitigations/controls.

7.1 Analysts preparing an SAA shall:

a. Consolidate the complementary safety and reliability analyses when two or more analyses were completed for the system (see Section 3.2.6).

b. Describe the system with sufficient detail to understand the intricacies of the system, including system design, operation, subsystem functions, operating location, and operating environment.

(1) List all of the ground rules and assumptions that were used in the analyses.

(2) Identify whether the system is safety critical, mission critical, or both.

(3) Include a summary of the quantity of CIs per criticality category, the quantity and type of hazard reports, and the quantity and criticality category of any flexible hoses, orifices, and/or filters from their respective FMEA analyses.

(4) Document areas of concern for the system design and its operation which may need to be resolved.

(5) Include a documentation list (e.g., reference documents, drawings) for all analyses included in the package.

(6) Include references to or incorporate software analyses performed for the system.

(7) Include references to related system analyses (O&SHA, GORA, HR, etc.) when hazard or failure information is related to the system.

APPENDIX A: DEFINITIONS

Accepted (Risk) Hazard: Risk associated with a hazard that has been accepted by the appropriate approval authority.

Approval: Formal documentation of agreement and authority to proceed as documented as long as the appropriate authority accepts any increase in risk.

Can: Used to denote discretionary privilege or permission.

Catastrophic: A condition that may cause death or permanent disability, loss of essential facilities, systems, equipment, or flight hardware. Note: A program/project may have different definitions of catastrophic.

Closed-Loop Tracking (Accounting): Accounting system that ensures traceability of CI/hazard controls by establishing operations and maintenance requirements, incorporating and uniquely identifying said requirements into the proper work documentation, and verifying that required operations and maintenance activities are performed and the requirements satisfied and closed out.

Commercial Off the Shelf (COTS): Commercial items that require no unique Government modification or maintenance over the life cycle of the product to meet the needs of the procuring agency. A commercial item is one customarily used for non-Governmental purposes that has been or will be sold, leased, or licensed (or offered for sale, lease, or license) in quantity to the general public.

Common Cause Failure (CCF): A failure of two or more components, subsystems, or structures due to a single specific event which bypasses or invalidates redundancy or independence.

Common Cause Failure Analysis (CCFA): An extension of FTA to identify "coupling factors" that can cause component failures to be potentially interdependent. Primary events of minimal cut sets from the FTA are examined through the development of matrices to determine if failures are linked to some common cause relating to environment, location, secondary causes, human error, or quality control.

Component: A combination of parts, devices, and structures, usually self-contained, which perform a distinctive function in the operation of the overall equipment.

Concurrence: Formal documentation of agreement with no authority to approve or accept risk.

Condition: Any as-found state, whether or not resulting from an event, that may have safety and/or mission assurance implications.

Consequence: An assessment of the worst-case credible potential effect(s) of a risk without any controls in place that is documented in terms of a consequence/severity level using the applicable risk matrix.

Consensus Standard: Standards developed or adopted by voluntary consensus standards bodies, both domestic and international.

Controlled (Risk) Hazard: Risk associated with a hazard where the likelihood of occurrence has been reduced to the lowest likelihood level in the applicable risk matrix.

Conventional Facilities: Basic dwellings used for commercial purposes such as an office building with multiple offices or tenants, mechanical rooms, utility rooms, restrooms, break rooms, classrooms, or a cafeteria.

Correcting Action: Actions, automatic or manual, which could be taken to circumvent a failure, to preclude occurrence of an identified hazard, or to prevent recurrence of a problem.

Credible: A condition that can occur and is reasonably likely to occur. If numeric data is available, conditions or failure modes with a probably of occurrence greater than 1×10^{-6} (1 in 1,000,000) in the projected usage/life of the equipment are credible. The probability of occurrence can change based on the program/project/Institution.

Critical: Any condition that could result in a Level 4 or 5 consequence per Section 5.2.1.

Critical Function: A system function which, if lost or improperly performed could result in a Level 4 or 5 consequence per Section 5.2.1.

Critical System: A system that has at least one critical function whose loss of function or improper performance could result in a critical condition.

Critical Item (CI): A component/LRU that does not meet failure tolerance requirements (i.e., fails a Failure Tolerance Screen). Criticality Category 1, 1R#, 1S, and 2 items are CIs; Criticality Category 3 items meet failure tolerance requirements.

Critical Items List (CIL): A searchable database which consolidates the CI reports that were generated as a result of the FMEA.

Critical Item (CI) Report: A report which documents the existence of a CI that contains specific rationale that justifies the retention of the CI in the system.

Criticality: A Program/project/Institution-defined measure of the consequence of a failure mode. Criticality of a system is determined by S&MA analysis of the function and application of the equipment. The classifications assigned to the system will guide the design team in determining which specifications and standards to apply, which materials to select, and how to document the system.

Criticality Assessment (CA): An analysis of each system input and output function to determine if the loss or improper performance of the function could result in a safety and/or mission critical failure. Functions that are determined to be safety and/or mission critical may receive further analysis in an FMEA. If the function is determined to be non-critical, an FMEA will not be performed.

Downstream System: A system that receives an input from the system being analyzed either directly or through intermediate systems.

Effect: A description of the potential worst-case results of a hazardous condition or failure mode.

Element: An essential part or component that is used to meet mission goals and objectives. Two or more elements usually interface to provide capabilities that they could not provide entirely by themselves. A mobile launch platform and tower would be considered an element while the launch vehicle would be considered a different element that would interface with each other.

Eliminated Hazard: A hazard that has been eliminated by completely removing the hazard causal factors.

End-to-End Review: A review which crosses subsystem boundaries to determine if interactions between all subsystems whose functional failures can cause hazards equivalent to Level 4 or 5 in the applicable risk matrix have been analyzed appropriately.

Failure: The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration.

Failure Mode: A description of the manner in which an item can fail.

Failure Modes and Effects Analysis (FMEA): A deductive, systematic, methodical analysis of the components that contribute to a system's critical functions which identifies and documents the worst-case effects of the component failure modes, hazards, and SFPs in regards to redundancy (or lack of redundancy).

Failure Tolerance: The ability for a system to meet its performance requirements after sustaining a failure.

Fault Tree Analysis (FTA): An inductive, analytical top-down analysis technique used to find all of the events and combinations of events that can lead to a top, undesired event (see Fault Tree Handbook with Aerospace Applications).

Flight Hardware: Hardware intended for launch into space, including payloads, manned or unmanned mission components, adapters, engines, launch vehicles, boosters, fuel tanks, etc.

Ground Operations Risk Assessment (GORA): A high-level risk assessment for ground processing involving a facility, ground system, flight hardware, environment, timing, a process, and/or processes. The hazards are determined by and are analyzed by a diverse team of knowledge experts and then reviewed by the affected management for risk-informed management decisions.

Hazard: A condition that has the potential to result in or contribute to injury, death, or equipment damage.

Hazard Analysis (HA): A detailed analysis that corresponds to the gates and events contained within a FTA which documents the existing and potential hazards and their recommended mitigations/controls. It details the mitigations/controls and verifications as well as the worst-case hazard risk scores using the Hazard Risk Matrix It also provides part of the certification rationale that will be used in the design certification report to support first-use of the system.

Hazard Report (HR): The output of a Hazard Analysis for a specific hazard whose risk is above the defined HR risk threshold. The HR documents the specific hazard, describes its causes, documents the controls and verifications, and states the current report status.

Hazardous Attribute: An inherent characteristic of a system which could result in a hazard.

Institution: A non-programmatic authority consisting of infrastructure, information technology, personnel, assets, and capabilities necessary to support mission success. The institution maintains responsibility for site planning, construction of new and maintenance of existing facilities, traffic ways, bridges, and utilities that can be used in support of programs or projects.

Integrated Hazard Analysis (IHA): Identification and evaluation of existing and potential hazards across two or more elements or interfacing systems containing the recommended mitigations for the hazard sources.

Interface: The point or area where a relationship exists between two or more parts, systems, programs, persons, or procedures where physical or functional compatibility is required.

Like Redundancy: Identical hardware items performing the same function.

Likelihood of Occurrence: An assessment of the likelihood or probability of a hazard's most severe effects transpiring. Likelihood takes into account that the hazard controls are in place and effective.

Line Replaceable Unit (LRU): An item whose replacement constitutes the optimum organizational maintenance repair action for a higher indenture item, i.e., any assembly which can be removed and replaced as a unit from the system at the operating location.

Mission Critical: A term used to identify a system that if failed (fault/failure) or produces improper system performance could result in a Level 4 or 5 consequence per Section 5.2.1 (people need not be present). This designation is dependent on the mission and objectives of the system as defined by the owning organization.

Non-credible Failure Mode: A failure that is considered to have a probability/likelihood of less than 10^{-6} of occurring during the lifetime of the system but cannot be considered completely eliminated due to a multitude of internal and external variables that could potentially precipitate the failure (e.g., the operating environment, maintenance, installation, wear, workmanship, wildlife, etc.).

Operating and Support Hazard Analysis (O&SHA): An analysis performed to identify hazards and recommend risk reduction alternatives in procedurally controlled activities during all phases of intended use. This work-step-by-work-step analysis focuses on identifying and evaluating hazards associated with the peripheral interaction of the system/element throughout the operation. These peripherals include environment, personnel, procedures, and equipment.

Operational Redundancy: Redundant hardware items, all of which are fully energized during the subsystem operating cycle. Operational redundancy includes load sharing hardware items connected in such a manner that, upon failure of one item, the remaining redundant items will continue to perform the subsystem function. Switching out the failed item is not required.

Passive Component: A component that may be necessary to the performance or structural integrity of a system but that does not change state during the performance of critical functions, or is a static structural member (i.e. passive structural components, pipes, flanges, manual valves used only for system configuration prior to operation, etc.).

Preliminary Hazard Analysis (PHA): A preliminary identification and evaluation of existing and potential hazards of a system and the recommended mitigation for the hazard sources found. The PHA is typically performed during the conceptual design phase.

Redundancy: Multiple ways of performing a function; several types of redundancy are commonly referenced, including Operational Redundancy, Standby Redundancy, Like Redundancy, and Unlike Redundancy.

Reliability: The probability that a system will not fail for a given period of time under specified operating and environmental conditions. Reliability is an inherent system design characteristic. As a principal contributing factor in operations and support costs and in system effectiveness, reliability plays a key role in determining the system's cost-effectiveness.

Reliability and Safety Assessment Report (RSAR): Typically, a one to two page safety and reliability assessment that is used to determine whether further safety and reliability analyses are necessary to support the design. The RSAR is comprised of a comprehensive, high-level system description summary (abstract) and states the system's high-level function/purpose and whether the system is safety critical, mission critical, both, or neither. It also states whether the system has software, and it includes specific rationale for performing or not performing further safety and/or reliability analyses.

Residual Risk: Risk that remains from a hazard after mitigations/controls have been applied.

Risk: The potential for performance shortfalls, which may be realized in the future, with respect to achieving explicitly, established and stated performance requirements. The performance shortfalls may be related to any one or more of the following mission execution domains: (1) safety, (2) technical, (3) cost, and (4) schedule. Risk is communicated using a combination of the likelihood (qualitative or quantitative) that an undesirable event will occur and the consequence/severity of the undesired event were it to occur. (See NPR 8000.4, Agency Risk Management Procedural Requirements.)

Risk Assessment: An evaluation of a risk that determines: (1) what can go wrong, (2) how likely is it to occur, (3) what the consequences are, (4) what the uncertainties are that are associated with the likelihood and consequences, and (5) what the mitigation plans are.

Risk Matrix: A table that defines levels of probability (Likelihood) and impact (Severity/Consequence) for either deterministic or risk-informed decision making.

Safety Critical: A term used to describe a condition, event, operation, process, equipment, or system that could result in a Level 4 or 5 consequence per Section 5.2.1 affecting people if performed or built improperly or allowed to remain uncorrected.

Safety Factor: Ratio of the design limit to the maximum operating conditions.

Severity: An assessment of the credible potential effect(s) of a risk without any controls in place (worst-case effects) that is documented in terms of a consequence level using the applicable matrix.

Shall: A mandatory action. Noncompliance with a "shall" statement requires approval of a request for relief.

Should: Used to denote a statement is good practice and is recommended, but not required (guidance). The advisability of a “should” statement depends on the specific facts in a given situation. Implementation of a “should” statement is at the discretion of the responsible KSC program/project or directorate organization.

Software: Computer programs developed to operate, control, service, or check out systems.

Software Assurance Classification Assessment (SACA): An assessment used to identify and evaluate the characteristics of software to determine the software's classification and the level of software assurance to be applied.

Standby Redundancy: Redundant hardware items that are non-operative (have no power applied) until they are switched into the subsystem upon failure of the primary item. Switching can be accomplished by either automatic or manual means.

System: The combination of elements that function together to produce the capability required to meet a need. The elements include all hardware, software, equipment, facilities, personnel, processes, and procedures needed for this purpose.

System Hazard Analysis (SHA): An analysis used to identify and evaluate existing and potential hazards of a system and the recommended mitigation for the hazard sources found. This analysis does not include a FTA. Identifies existing and potential hazards from the functional relationships between components and equipment comprising each subsystem.

System Safety: Application of engineering and management principles, criteria, and techniques to prevent and avoid hazards within the constraints of operational effectiveness, time, and cost throughout all phases of the system/software life cycle.

Subsystem: An element of a system that in itself may constitute a system.

System Functional Block Diagram: A graphical block diagram that describes the interrelationships of a system’s or subsystems’ inputs and outputs.

Time-to-Correct: An estimate of time or time range once a failure has been detected to correct the situation.

Time-to-Detect: An estimate of the time from failure initiation to when the failure is detectable.

Time-to-Effect: An estimate of the time from failure occurrence to manifestation of the worst-case failure effect.

Tools: Equipment designed for general use in a variety of applications. Tools are calibrated, when necessary, in accordance with industry standards. Tools are not designed to specifically interface with flight hardware; however their design and general use includes a variety of applications that may also include flight hardware or system. Tools are intended for use by trained technicians and facilitate manual operations, such as torqueing fasteners, cutting wire, checking electrical continuity, and verifying surface clearances.

Unlike Redundancy: Non-identical hardware items performing the same function. Safety features which provide protection for specific failure modes are considered as unlike redundancy for that failure mode; i.e., relief valves which provide protection against over-

pressurization after failure of a regulator, transducers, and associated software which provide redline protection.

Upstream System: A system that provides an input to the system being analyzed either directly or through intermediate systems.

Will: Used to denote an expected outcome.

Worst-Case Effects: The absolute worst outcome that could possibly result under the specified conditions.

APPENDIX B: ABBREVIATIONS AND ACRONYMS

=	Equals
>	Greater Than
#	Number
-	Negative
x	by
X	Multiplication
CA	Criticality Assessment
CCF	Common Cause Failure
CCFA	Common Cause Failure Analysis
CD	Center Director
CDR	Critical Design Review
CI	Critical Item
CIL	Critical Items List
COTS	Commercial Off-the-Shelf
Crit.	Criticality Category
DFMR	Design for Minimum Risk
E	Eliminated
e.g.	For example
EPA	Environmental Protection Agency
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
GORA	Ground Operations Risk Assessment
GRRP	Ground Risk Review Panel
HA	Hazard Analysis
HR	Hazard Report
i.e.	In-other-words
IHA	Integrated Hazard Analysis
JHA	Job Hazard Analysis
KDP	Kennedy Documented Procedures
KNPD	Kennedy NASA Procedural Directive
KNPR	Kennedy NASA Procedural Requirements
KSC	Kennedy Space Center
LRU	Line Replaceable Unit
N/A	not applicable
NASA	National Aeronautics and Space Administration
NPD	NASA Procedural Directive
NPR	NASA Procedural Requirement

O&SHA	Operating and Support Hazard Analysis
PHA	Preliminary Hazard Analysis
PLC	Programmable Logic Controller
PLN	Plan
PMN	Program Model Number
Rev.	Revision
RSAR	Reliability and Safety Assessment Report
S&MA	Safety and Mission Assurance
SAA	System Assurance Analysis
SACA	Software Assurance Classification Assessment
SFP	Single Failure Point
SHA	System Hazard Analysis
UG	User's Guide

APPENDIX C: REFERENCE DOCUMENTS

C.1 NPD 7120.4, NASA Engineering and Program/Project Management Policy

C.2 NPR 7120.7, Institutional Infrastructure and Information Technology Program and Project Management

C.3 NPR 8000.4, Agency Risk Management Procedural Requirements

C.4 NPR 8831.2, Facilities Maintenance and Operations Management

C.5 NASA-STD-5005, Standard for the Design and Fabrication of Ground Support Equipment

C.6 NASA-STD-8719.11, NASA Safety Standard for Fire Protection

C.7 NASA-STD-8719.13, Software Safety Standard

C.8 KNPD 8700.1, Safety and Mission Assurance Policy Directive

C.9 KDP-KSC-P-3221, JHA Selection

C.10 KSC-STD-DE-512-SM, Facility Systems, Ground Support Systems, and Ground Support Equipment General Design Requirements

C.11 KSC-UG-2816, Institutional Safety and Mission Assurance Division Safety Checklist, Example and Template User Guide